

EXHIBIT M

**UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549**

FORM 10-Q

(Mark One)

☒ **QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the quarterly period ended March 31, 2022

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from _____ to _____

Commission File Number: 001-37622

Block, Inc.

(Exact name of registrant as specified in its charter)

Delaware

(State or other jurisdiction of
incorporation or organization)

80-0429876

(IRS Employer
Identification No.)

Address Not Applicable¹

(Address of principal executive offices, including zip code)

(415) 375-3176

(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Trading Symbol(s)	Name of each exchange on which registered
Class A common stock, \$0.0000001 par value per share	SQ	New York Stock Exchange

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒ Accelerated filer ☐ Non-accelerated filer ☐ Smaller reporting company ☐ Emerging growth company ☐

¹ We do not designate a headquarters location as we have adopted a distributed work model.

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

As of April 29, 2022, the number of shares of the registrant's Class A common stock outstanding was 518,807,380 and the number of shares of the registrant's Class B common stock outstanding was 61,696,578.

Item 1A. Risk Factors

Investing in our securities involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Quarterly Report on Form 10-Q, including the section titled “Management’s Discussion and Analysis of Financial Condition and Results of Operations” and our condensed consolidated financial statements and related notes, before making any investment decision with respect to our securities. The risks and uncertainties described below may not be the only ones we face. If any of the risks actually occur, our business could be materially and adversely affected. In that event, the market price of our Class A common stock could decline, and you could lose part or all of your investment.

The following description of risk factors includes any material changes to, and supersedes the description of, risk factors associated with the Company’s business previously disclosed in Part I, Item 1A of our Annual Report on Form 10-K for the fiscal year ended December 31, 2021 under the heading “Risk Factors.”

Risk Factors Summary

Our business operations are subject to numerous risks and uncertainties, including those outside of our control, that could cause our actual results to be harmed, including risks regarding the following:

Risks related to our business and our industry:

- our ability to maintain, protect, and enhance our brands;
- our participation in government relief programs set up in response to the COVID-19 pandemic;
- our ability to retain existing sellers and customers, attract new sellers and customers, and increase sales to both new and existing sellers and customers;
- our investments in our business and ability to maintain profitability;
- our efforts to expand our product portfolio and market reach;
- our ability to develop products and services to address the rapidly evolving market for payments and financial services;
- competition in our industry;
- any acquisitions, strategic investments, entries into new businesses, joint ventures, divestitures and other transactions that we may undertake;
- liabilities that may exist at Afterpay;
- the successful integration of our business with Afterpay;
- additional risks of our majority interest in TIDAL;
- expanding our business globally;
- additional risks of BNPL lending;
- additional risks of Square Banking relating to the structure of bank partnerships, and FDIC and other regulatory obligations; and
- additional risks of Square Loans related to the availability of capital, seller payments, interest rate, deposit insurance premiums, and general macroeconomic conditions.

Operational risks:

- real or perceived improper or unauthorized use of, disclosure of, or access to sensitive data;
- real or perceived security breaches or incidents or human error in administering our software, hardware, and systems;
- systems failures, interruptions, delays in service, catastrophic events, and resulting interruptions in the availability of our products or services or those of our sellers;
- any inability to access our private keys required to access our bitcoins or any hack or other data loss relating to the bitcoins we hold;
- our risk management efforts;
- our dependence on payment card networks and acquiring processors;
- our reliance on third parties and their systems for a variety of services, including the processing of transaction data and settlement of funds;
- our dependence on key management and any failure to attract, motivate, and retain our employees;
- our operational, financial, and other internal controls and systems;
- any shortage, price increases, tariffs, changes, delay or discontinuation of our key components;
- our ability to accurately forecast demand for our products and adequately manage our product inventory;
- the integration of our services with a variety of operating systems and the interoperation of our hardware that enables merchants to accept payment cards with third-party mobile devices utilizing such operating systems; and
- difficulties estimating the amount payable under TIDAL’s license agreements.

Economic, financial, and tax risks:

- the ongoing COVID-19 pandemic and measures intended to prevent its spread;
- a deterioration of general macroeconomic conditions;
- any inability to secure financing on favorable terms, or at all, or covenants in our existing credit agreement, the indentures, or future agreements;
- our ability to service our convertible notes and our senior notes;
- counterparty risk with respect to our convertible note hedge transactions;
- our bitcoin investments being subject to volatile market prices, impairment, and other risks of loss;
- foreign exchange rates risks; and
- any greater-than-anticipated tax liabilities or significant valuation allowances on our deferred tax assets.

Legal, regulatory, and compliance risks:

- extensive regulation and oversight in a variety of areas of our business;
- complex and evolving regulations and oversight related to privacy and data protection;
- litigation, including intellectual property claims, government investigations or inquiries, and regulatory matters or disputes;
- obligations and restrictions as a licensed money transmitter;
- regulatory scrutiny or changes in the BNPL space;
- regulation and scrutiny of our subsidiary Cash App Investing, which is a broker-dealer registered with the SEC and a member of FINRA, including net capital and other regulatory capital requirements;
- changes to our business practices imposed by FINRA based on our ownership of Cash App Investing;
- regulation and scrutiny of our subsidiary Square Financial Services, which is a Utah state-chartered industrial bank, including the requirement that we serve as a source of financial strength to it;
- supervision and regulation of Square Financial Services, including the Dodd-Frank Act and its related regulations;
- any inability to protect our intellectual property rights; and
- assertions by third parties of infringement of intellectual property rights by us.

Risks related to ownership of our common stock:

- the dual class structure of our common stock;
- volatility of the market price of our Class A common stock;
- the dual-listing of our Class A common stock on the NYSE and our CDIs on the Australian Securities Exchange;
- our convertible note hedge and warrant transactions;
- anti-takeover provisions contained in our amended and restated certificate of incorporation, our second amended and restated bylaws, and provisions of Delaware law; and
- exclusive forum provisions in our bylaws.

Risks Related to Our Business and Our Industry***Our business depends on our ability to maintain, protect, and enhance our brands.***

Having a strong and trusted brand has contributed significantly to the success of our business. We believe that maintaining, promoting, and enhancing the Square brand, the Cash App brand, the TIDAL brand, and our other brands, in a cost-effective manner is critical to achieving widespread acceptance of our products and services and expanding our base of customers. Maintaining and promoting our brands will depend largely on our ability to continue to provide useful, reliable, secure, and innovative products and services, as well as our ability to maintain trust and be a technology leader. We may introduce, or make changes to, features, products, services, privacy practices, or terms of service that customers do not like, which may materially and adversely affect our brands. Our brand promotion activities may not generate customer awareness or increase revenue, and even if they do, any increase in revenue may not offset the expenses we incur in building our brands. If we fail to successfully promote and maintain our brands or if we incur excessive expenses in this effort, our business could be materially and adversely affected.

The introduction and promotion of new products and services, as well as the promotion of existing products and services, may be partly dependent on our visibility on third-party advertising platforms, such as Google, Twitter, or Facebook. Changes in the way these platforms operate or changes in their advertising prices, data use practices or other terms could make the maintenance and promotion of our products and services and our brands more expensive or more difficult. If we are unable to market and promote our brands on third-party platforms effectively, our ability to acquire new customers would be materially harmed. We also use retail partners to sell hardware and acquire sellers for Square. Our ability to acquire new

We have experienced and will likely continue to experience denial-of-service and other cyber-attacks, system failures, outages, security incidents, and other events or conditions that interrupt the availability, data integrity, or reduce the speed or functionality of our products and services. These events have resulted and likely will result in loss of revenue. In addition, they could result in significant expense to repair or replace damaged equipment and remedy resultant data loss or corruption. The risk of cybersecurity incidents is increasing as we experience an increase in electronic payments, e-commerce, and other online activity. Additionally, due to political uncertainty and military actions associated with Russia's invasion of Ukraine, we and our service providers are vulnerable to heightened risks of cybersecurity incidents and security and privacy breaches from or affiliated with nation-state actors, including attacks that could materially disrupt our systems, operations, supply chain, products, and services. We cannot provide assurances that our preventative efforts against such incidents will be successful. A prolonged interruption in the availability or reduction in the speed or other functionality of our products or services could materially harm our reputation and business. Frequent or persistent interruptions in our products and services could cause customers to believe that our products and services are unreliable, leading them to switch to our competitors or to avoid our products and services, and could permanently harm our reputation and business. Moreover, to the extent that any system failure or similar event results in damages to customers or contractual counterparties, these customers and contractual counterparties could seek compensation from us for their losses, and those claims, even if unsuccessful, would likely be time-consuming and costly for us to address.

A significant natural or man-made disaster could have a material and adverse impact on our business. Certain of our offices and data center facilities are located in the San Francisco Bay Area, a region known for seismic activity. Despite any precautions we may take, the occurrence of a natural disaster or other unanticipated problems at our offices or data centers could result in lengthy interruptions in our services or could result in related liabilities. We do not maintain insurance sufficient to compensate us for the potentially significant losses that could result from disruptions to our services.

Significant natural or other disasters, including pandemics, could also have a material and adverse impact on our sellers or other customers, which, in the aggregate, could in turn adversely affect our results of operations.

The loss or destruction of a private key required to access our bitcoin may be irreversible. If we are unable to access our private keys or if we experience a hack or other data loss relating to the bitcoins we hold on behalf of ourselves and our customers, we and our customers may be unable to access such bitcoins and it could harm customer trust in us and our products.

Bitcoins are controllable only by the possessor of both the unique public key and private key relating to the local or online digital wallet in which the bitcoins are held. While the bitcoin and blockchain ledger require a public key relating to a digital wallet to be published when used in a transaction, private keys must be safeguarded and kept private in order to prevent a third-party from accessing the bitcoins held in such digital wallet. To the extent any of our private keys are lost, destroyed, or otherwise compromised and no backup of such private key is accessible, we will be unable to access the bitcoins held in the related digital wallet. Additionally, we use a third-party custodian to store a portion of our bitcoins in an offline and air-gapped cold storage. Any inappropriate access or theft of bitcoins held by our custodian, or the custodian's failure to maintain effective controls over the custody and other settlement services provided to us, could materially and adversely affect us. We cannot provide assurance that the digital wallets used to store our and our customers' bitcoins will not be hacked or compromised. The bitcoin and blockchain ledger, as well as other cryptocurrencies and blockchain technologies, have been, and may in the future be, subject to security breaches or incidents, hacking, or other malicious activities. Any loss of private keys relating to, or hack or other compromise of, digital wallets used to store our customers' bitcoins could adversely affect our customers' ability to access or sell their bitcoins and could harm customer trust in us and our products, require us to expend significant funds for remediation, and expose us to litigation and other potential liability. Additionally, any loss of private keys relating to, or hack or other compromise of, digital wallets used by third parties to store bitcoins or other cryptocurrencies could have negative reputational effects on us and harm customer trust in us and our products. As the number of customers who use our bitcoin product has increased and the value of bitcoins we hold on behalf of such customers has grown significantly, the risks and consequences of such adverse events have increased and could materially and adversely affect our business.

Our risk management efforts may not be effective, which could expose us to losses and liability and otherwise harm our business.

We offer payments and other products and services to a large number of customers. We have programs to vet and monitor these customers and the transactions we process for them as part of our risk management efforts, but such programs require continuous improvement and may not be effective in detecting and preventing fraud and illegitimate transactions. When our payments services are used to process illegitimate transactions, and we settle those funds to customers and are

unable to recover them, we suffer losses and liability. As a greater number of larger sellers use our services, our exposure to material risk losses from a single seller, or from a small number of sellers, will increase. Illegitimate transactions can also expose us to governmental and regulatory enforcement actions and potentially prevent us from satisfying our contractual obligations to our third-party partners, which may cause us to be in breach of our obligations. The highly automated nature of, and liquidity offered by, our payments and peer-to-peer services make us and our customers a target for illegal or improper uses, including scams and fraud directed at Cash App customers, fraudulent or illegal sales of goods or services, money laundering, and terrorist financing. Identity thieves and those committing fraud using stolen or fabricated credit card, debit card, or bank account numbers, or other deceptive or malicious practices, potentially can steal significant amounts of money from businesses like ours or from our customers or third parties. Our risk management policies, procedures, techniques, and processes may not be sufficient to identify all of the risks to which we are exposed, to enable us to prevent or mitigate the risks we have identified, or to identify additional risks to which we may become subject in the future. Our current business, changes due to COVID-19 and the related economic impact, and anticipated domestic and international growth will continue to place significant demands on our risk management and compliance efforts, and we will need to continue developing and improving our existing risk management infrastructure, techniques, and processes. In addition, when we introduce new services, such as Square Banking and BNPL, expand existing services, including online payment acceptance, focus on new business areas, including consumer financing and loans, or begin to operate in markets where we have a limited history of fraud loss, we may be less able to forecast and carry appropriate reserves on our books for those losses. Additionally, we recently launched Cash App Teens, making certain Cash App functions, such as Cash Card, limited peer-to-peer payments, and direct deposits available to teenagers between the ages of 13 through 17 with the authorization of a parent or guardian. The risks and the potential harm to our reputation are magnified in instances of fraud or unauthorized or inappropriate transactions involving minors.

While we maintain a program of insurance coverage for various types of liabilities, we may self-insure against certain business risks and expenses where we believe we can adequately self-insure against the anticipated exposure and risk or where insurance is either not deemed cost-effective or unavailable.

We are currently, and will continue to be, exposed to risks associated with chargebacks and refunds in connection with payment card fraud or relating to the goods or services provided by our sellers. In the event that a billing dispute between a cardholder and a seller is not resolved in favor of the seller, including in situations where the seller engaged in fraud, the transaction is typically “charged back” to the seller and the purchase price is credited or otherwise refunded to the cardholder. The risk of chargebacks is typically greater with our sellers that promise future delivery of goods and services. Moreover, chargebacks typically increase during economic downturns due to sellers becoming insolvent or bankrupt or otherwise unable to fulfill their commitments for goods or services. Additionally, the recent global supply chain disruptions and shortages related to the COVID-19 pandemic have negatively affected sellers’ ability to deliver goods and services on time or at all, which increases the risk of chargebacks. If we are unable to collect chargebacks or refunds from the seller’s account, or if the seller refuses to or is unable to reimburse us for chargebacks or refunds due to closure, bankruptcy, or other reasons, we, as the merchant of record, may bear the loss for the amounts paid to the cardholder. We collect and hold reserves for a limited number of sellers whose businesses are deemed higher risk in order to help cover potential losses from chargebacks and refunds, but this practice is limited and there can be no assurances that we will be successful in mitigating such losses. Our financial results would be adversely affected to the extent sellers do not fully reimburse us for the related chargebacks and refunds. Moreover, since October 2015, businesses that cannot process EMV chip cards are held financially responsible for certain fraudulent transactions conducted using chip-enabled cards. Not all of the readers we offer to merchants are EMV-compliant. If we are unable to maintain our losses from chargebacks at acceptable levels, the payment card networks could fine us, increase our transaction-based fees, or terminate our ability to process payment cards. Any increase in our transaction-based fees could damage our business, and if we were unable to accept payment cards, our business would be materially and adversely affected. If any of our risk management policies and processes, including self-insurance or holding seller reserves, are ineffective, we may suffer large financial losses, we may be subject to civil and criminal liability, and our business may be materially and adversely affected.

We are dependent on payment card networks and acquiring processors, and any changes to their rules or practices could harm our business.

Our business depends on our ability to accept credit and debit cards, and this ability is provided by the payment card networks, including Visa, MasterCard, American Express, and Discover. In a majority of these cases, we do not directly access the payment card networks that enable our acceptance of payment cards. As a result, we must rely on banks and acquiring processors to process transactions on our behalf. These banks and acquiring processors may fail or refuse to process transactions adequately, may breach their agreements with us, or may refuse to renegotiate or renew these agreements on terms that are favorable or commercially reasonable. They might also take actions that degrade the functionality of our services, impose additional costs or requirements on us, or give preferential treatment to competitive services, including their own

Our future success is significantly dependent upon the continued service of our executives and other key employees. If we lose the services of any member of management or any key personnel, we may not be able to locate a suitable or qualified replacement, and we may incur additional expenses to recruit and train a replacement, which could severely disrupt our business and growth.

To maintain and grow our business, we will need to identify, attract, hire, develop, motivate, and retain highly skilled employees. This requires significant time, expense, and attention. In addition, from time to time, there may be changes in our management team that may be disruptive to our business. If our management team, including any new hires that we make, fails to work together effectively and to execute our plans and strategies on a timely basis, our business could be harmed. Competition for highly skilled personnel is intense, particularly in the San Francisco Bay Area where some of our offices are located. We may need to invest significant amounts of cash and equity to attract and retain new employees, and we may never realize returns on these investments. Additionally, potential changes in U.S. immigration policy may make it difficult to renew or obtain visas for any highly skilled personnel that we have hired or are actively recruiting. Furthermore, our international expansion and our business in general may be materially adversely affected if legislative or administrative changes to immigration or visa laws and regulations impair our hiring processes or projects involving personnel who are not citizens of the country where the work is to be performed. If we are not able to add and retain employees effectively, our ability to achieve our strategic objectives will be adversely affected, and our business and growth prospects will be harmed.

If we do not continue to improve our operational, financial, and other internal controls and systems to manage growth effectively, our business could be harmed.

Our current business and anticipated growth, as well as our entry into new lines of business and our acquisitions, will continue to place significant demands on our management and other resources. In order to manage our growth effectively, we must continue to strengthen our existing infrastructure and operational procedures, enhance our internal controls and reporting systems, and ensure we timely and accurately address issues as they arise. In particular, our continued growth will increase the challenges involved in:

- improving existing and developing new internal administrative infrastructure, particularly our operational, financial, communications, and other internal systems and procedures;
- successfully expanding and implementing internal controls as they relate to our new lines of business and any acquired businesses;
- installing enhanced management information and control systems; and
- preserving our core values, strategies, and goals and effectively communicating these to our employees worldwide.

These challenges have increased as we shift to a more distributed workforce. If we are not successful in developing and implementing the right processes and tools to manage our enterprise, our ability to compete successfully and achieve our business objectives could be impaired.

These efforts may require substantial financial expenditures, commitments of resources, developments of our processes, and other investments and innovations. As we grow and our business model evolves, we must balance the need for additional controls and systems with the ability to efficiently develop and launch new features for our products and services. However, it is likely that as we grow, we will not be able to launch new features, or respond to customer or market demands as quickly as a smaller, more efficient organization. If we do not successfully manage our growth, our business will suffer.

Additionally, our key metrics are calculated using internal company data based on the activity we measure on our platforms and may be compiled from multiple systems, including systems that are organically developed or acquired through business combinations. There are inherent challenges and limitations in measuring our business globally at scale, and the methodologies used to calculate our key metrics inherently require some judgment. For example, we currently identify a Cash App transacting active as a Cash App account that has at least one financial transaction using any product or service within Cash App during a specified period although certain of these accounts may share an alias identifier with one or more other transacting active accounts (for example, families sharing one alias identifier or one customer with multiple accounts). We regularly review our processes for calculating these key metrics, and from time to time we may make adjustments to improve their accuracy or relevance. Further, as our business develops, we may revise or cease reporting metrics if we determine that such metrics are no longer appropriate measures of our performance. If investors do not consider our reporting metrics to accurately reflect our business or they disagree with our methodologies, our reputation may be harmed and our business may be adversely impacted.

particularly as we expand into new areas of operations, which could have a significant negative effect on our existing business and our ability to pursue future plans.

Laws, regulations, and standards are subject to changes and evolving interpretations and application, including by means of legislative changes and/or executive orders, and it can be difficult to predict how they may be applied to our business and the way we conduct our operations, particularly as we introduce new products and services and expand into new jurisdictions.

For example, Cash App includes a feature that permits our customers to buy and sell bitcoin. Bitcoin is not widely accepted as legal tender or backed by governments around the world, and it has experienced price volatility, technological glitches, security compromises, and various law enforcement and regulatory interventions. Certain existing laws also prohibit transactions with certain persons and entities, and we have a risk based program in place to prevent such transactions. Despite this, due to the nature of bitcoin technology and blockchain, it may be technically infeasible to prevent all such transactions, and there can be no guarantee that our measures will be viewed as sufficient. The regulation of cryptocurrency and crypto platforms is still an evolving area, and it is possible that we could become subject to additional regulations. If we fail to comply with regulations or prohibitions applicable to us, we could face regulatory or other enforcement actions and potential fines and other consequences. Further, we might not be able to continue operating the feature, at least in current form, which could cause the price of our Class A common stock to decrease.

We are subject to audits, inspections, inquiries, and investigations from regulators on an ongoing basis. Although we have a compliance program focused on the laws, rules, and regulations applicable to our business, we have been and may still be subject to inquiries, investigations, fines, or other penalties in one or more jurisdictions levied by regulators, including federal agencies, state Attorneys General and private plaintiffs who may be acting as private attorneys general pursuant to various applicable laws, as well as those levied by foreign regulators. In addition to fines, penalties for failing to comply with applicable rules and regulations could include significant criminal and civil lawsuits, forfeiture of significant assets, increased licensure requirements, revocation of licenses or other enforcement actions. We have been and may be required to make changes to our business practices or compliance programs as a result of regulatory scrutiny. In addition, any perceived or actual breach of compliance by us with respect to applicable laws, rules, and regulations could have a significant impact on our reputation as a trusted brand and could cause us to lose existing customers, prevent us from obtaining new customers, require us to expend significant funds to remedy problems caused by breaches and to avert further breaches, and expose us to legal risk and potential liability.

Further, from time to time, we may leverage third parties to help conduct our businesses in the U.S. or abroad. We and our third-party intermediaries may have direct or indirect interactions with officials and employees of government agencies or state-owned or affiliated entities and may be held liable for any corrupt or other illegal activities of these third-party business partners and intermediaries, our employees, partners, and agents, even if we do not explicitly authorize such activities. While we have policies and procedures to address compliance with such laws, we cannot assure you that our employees and agents will not take actions in violation of our policies and applicable law, for which we may be ultimately held responsible.

Our business is subject to complex and evolving regulations and oversight related to privacy, data protection, and data security.

We are subject to laws and regulations relating to the collection, use, retention, privacy, protection, security, and transfer of information, including personal information of our employees and customers. As with the other laws and regulations noted above, these laws and regulations may change or be interpreted and applied differently over time and from jurisdiction to jurisdiction, and it is possible they will be interpreted and applied in ways that will materially and adversely affect our business. For example, the European Union's General Data Protection Regulation ("GDPR") and similar legislation in the United Kingdom ("U.K.") impose stringent data privacy and data protection requirements and provide for greater penalties for noncompliance of up to the greater of 4% of worldwide annual revenue or €20 million or £17.5 million, as applicable. The GDPR restricts international data transfers from the EU to other jurisdictions unless the rights of the individual data subjects in respect of their personal data is protected by an approved transfer mechanism, or one of a limited number of exceptions applies. The U.K.'s data protection regime contains similar requirements. When transferring personal data from the EU to other jurisdictions, we utilize standard contractual clauses published by the EU Commission (the "SCCs"). On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued a decision that may impose additional obligations on companies when relying on those SCCs. This CJEU decision may result in different EEA data protection regulators applying differing standards for the transfer of personal data from the EEA to the United States, and even require ad hoc verification of measures taken with respect to data flows. As a result of this CJEU decision or other developments with respect to the legal and regulatory regime affecting cross-border data transfers, we may be required to take additional steps to legitimize impacted

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned thereunto duly authorized.

BLOCK, INC.

Date: May 5, 2022

By: /s/ Jack Dorsey

Jack Dorsey
Block Head and Chairperson
(Principal Executive Officer)

By: /s/ Amrita Ahuja

Amrita Ahuja
Chief Financial Officer
(Principal Financial Officer)